

# **Exhibit 6 –**

## **Declaration of**

### **Chris Riley (techpolicy.social)**

**IN THE UNITED STATES DISTRICT COURT  
FOR THE WESTERN DISTRICT OF TEXAS  
AUSTIN DIVISION**

COMPUTER & COMMUNICATIONS )  
INDUSTRY ASSOCIATION, and )  
 )  
NETCHOICE, LLC, )  
 )  
*Plaintiffs,* )  
 ) Civil Action No. 1:24-cv-849  
v. )  
 )  
KEN PAXTON, in his official capacity as )  
Attorney General of Texas, )  
 )  
*Defendant.* )

**DECLARATION OF CHRIS RILEY IN SUPPORT OF PLAINTIFFS'  
MOTION FOR PRELIMINARY INJUNCTION**

I, Chris Riley, declare as follows:

1. I am the Executive Director of the Data Transfer Initiative and a Distinguished Research Fellow at the Annenberg Public Policy Center at the University of Pennsylvania. I have previously worked for the R Street Institute, Brave New Software, Mozilla, the U.S. Department of State, as an attorney at the Federal Communications Commission, and as an adjunct professor at the American University School of International Service. I have a B.S. in Computer Science from Wheeling Jesuit University, a PhD in Computer Science from Johns Hopkins University, and a JD from Yale Law School. Most relevant here, I operate a website that I understand to potentially be subject to certain provisions in Texas House Bill 18, 2023 Tex. Sess. Law Serv. Ch. 795 (“HB18”), which will take effect September 1, 2024.

2. I submit this declaration in support of Plaintiffs’ Motion for a Preliminary Injunction. I am over the age of 18 and am competent to make the statements herein. I have

personal knowledge of the facts set forth in this declaration and, if called and sworn as a witness, could and would competently testify to them.

**I. techpolicy.social**

3. I am currently the sole operator of techpolicy.social, which is a website made up of technology and Internet policy professionals sharing their own user-generated content. The goal of techpolicy.social is to foster a community where those professionals can share information, discuss ideas, and foster offline collaboration through online engagement. Techpolicy.social currently has approximately 35 active members who are working in, or adjacent to, technology and Internet policy and who interact on techpolicy.social to discuss those topics. Techpolicy.social is accessible in Texas. Though techpolicy.social's community is unique, my experience in the field is that the Internet is full of similar websites centered around different communities of people with shared interests.

4. Techpolicy.social is one “instance” on Mastodon’s larger decentralized social network. I am one of many people that used Mastodon’s open-source software to create my own website where people can post, message, and build their own communities based on shared interests. Each instance is its own micro-blogging service with multiple “feeds” of content that look similar to feeds on other microblogging services like X (formerly known as Twitter). Mastodon instances all have “local feeds” with content specific to their communities, made up of posts from users in that specific instance. In other words, all techpolicy.social users see a feed exclusively made up of content posted by other techpolicy.social users. I have complete content-moderation control over the content in the local feed. But techpolicy.social users can also see a “federated” feed that includes content from many other Mastodon instances. That federated feed includes all posts from all accounts that members of techpolicy.social follow. *See Mastodon, Using the Network Features, <https://tinyurl.com/3tx282xn>* (“When you browse the federated timeline,

you see all public posts that the server you are on knows about.”). And the converse is also true: Users on other instances can see content from techpolicy.social in their federated feeds. Although I am able to curate the content that appears on techpolicy.social’s feed, I do not have complete content-moderation control over content in the federated feed or content on federated feeds in other instances.

5. Running my Mastodon instance is akin to being the sole-proprietor of a smaller social media website, where I alone have responsibility for management and content moderation. Unlike other social media companies, no company centrally controls all Mastodon instances. Below are some of my responsibilities:

**a. Users.** techpolicy.social is only open to registered users. Although anyone can see public posts on techpolicy.social, actual participation in the community is by request or invite only, and I screen any user seeking to be part of the community. To do so, I request that any user seeking admission give me personal identifying information through a reference link (*i.e.*, another public profile or a bio on an organizational website) so that I can determine whether the user will fit with the group and is a real person. If I cannot verify a user based on what information she has provided, I will follow up with that person to ensure that she is the person she represents herself to be. Although I try to verify that all users are real persons, I do allow some users into techpolicy.social who are pseudonymous, although I currently do not have pseudonymous users as far as I am aware. Verifying an average prospective user’s general identity can take me approximately an hour.

**b. Minors.** To the best of my knowledge, techpolicy.social has no minor users. However, I do not have a protocol for verifying the exact age of users. And because I allow users who operate under pseudonyms to enter the instances, I cannot be certain that all users on techpolicy.social are

over the age of 18. Plus, I may allow on users in the future who I know to be minors. Regardless, content from techpolicy.social may show up in minors' federated feeds on other instances.

**c. Content Moderation.** I am solely responsible for content-moderation enforcement. I have developed a content-moderation policy for techpolicy.social that governs permissible use on the website. Violating the content-moderation rules may result in removal from the techpolicy.social instance. My policy prohibits: (1) racism, sexism, homophobia, transphobia, xenophobia, and casteism; (2) incitement to violence or promotion of violent ideologies; (3) harassment, dogpiling, and doxxing; (4) intentionally false or misleading information; and (5) any content that is illegal under United States law, including child sexual abuse material (“CSAM”). Furthermore, any sexually explicit or violent media must be marked as sensitive; there is very little, if any, such content on techpolicy.social. I will remove content if I see that the content violates the instance’s policy or if another user reports it. I do not have any automated system for enforcing the content-moderation policy. There have been few situations in which I have had to enforce techpolicy.social’s content moderation policy. These situations have involved spam or some instances of harassment. I have never uncovered—and techpolicy.social users have never flagged—CSAM posted on techpolicy.social.

**d. Interaction With Other Mastodon Instances.** I also determine which other instances techpolicy.social users can interact with. I maintain a “block list” of instances that I know are hospitable to bad actors—primarily instances that promote cryptocurrency scams, drug sales, or other blatantly illegal conduct. If a user created an account through that instance, then that user cannot interact with any users of techpolicy.social, and vice versa.

**e. Costs of Maintaining the Website.** I pay for all costs associated with hosting techpolicy.social, although members can contribute to defray those costs. To date, user

contributions have come nowhere near covering the server costs to run the website. I spend approximately \$50.00 per month on server costs and if the costs of running the instance increased much more than that, I would consider shutting down techpolicy.social.

**II. Compliance with Texas House Bill 18 Threatens My Ability to Continue Operating techpolicy.social.**

6. It is my understanding that HB18 may cover techpolicy.social and my operation of the website as a “digital service provider.” Tex. Bus. & Com. Code § 509.001(2) (2024). techpolicy.social is a “digital service” that “(1) connects users in a manner that allows users to socially interact with other users on the digital service; (2) allows a user to create a public or semi-public profile for purposes of signing into and using the digital service; and (3) allows a user to create or post content that can be viewed by other users of the digital service, including sharing content on: (A) a message board; (B) a chat room; or (C) a landing page, video channel, or main feed that presents to a user content created and posted by other users.” *Id.* §§ 509.001(1), 509.002(a). Based on my understanding, HB18 provides no exception for small websites with user-generated content like techpolicy.social. To the best of my knowledge, then, techpolicy.social may be required to comply with HB18’s requirements.

7. Although I currently moderate techpolicy.social and do not have minor users on techpolicy.social that I know of, given the breadth of the law, I believe that HB18 will require me to implement additional content-moderation technology and efforts that would be cost- and time-prohibitive for a sole proprietor of a small website to implement. These additional costs and the inherent uncertainty in how the law applies to small-scale digital service providers like me will lead me to consider shutting down techpolicy.social rather than shoulder these compliance costs or run the risk of potential liability. Shutting down techpolicy.social would deprive me and the

website's users from a community of like-minded people interested in technology and Internet policy.

8. Primarily, HB18's requirement that digital service providers "develop and implement a strategy to prevent [a] known minor's exposure to" certain enumerated content would be cost- and time-prohibitive to adopt for a small website like mine. *Id.* § 509.053(a). That section requires digital service providers to adopt the following mandatory technical requirements: "(A) creating and maintaining a comprehensive list of [certain content] to block from display to a known minor; (B) using filtering technology and other protocols to enforce the blocking of [certain content]; (C) using hash-sharing technology and other protocols to identify recurring [certain content]; (D) creating and maintaining a database of keywords used for filter evasion, such as identifiable misspellings, hash-tags, or identifiable homoglyphs; (E) performing standard human-performed monitoring reviews to ensure efficacy of filtering technology; (F) making available to users a comprehensive description of the categories of [certain content] that will be filtered; and (G) except as provided by Section 509.058, making available the digital service provider's algorithm code to independent security researchers." *Id.* § 509.053(b). Technology like "hash-sharing" and "filtering technology"—and the infrastructure to support it—is expensive and largely unavailable to small websites like mine. Even if such technology were easily available, because I am the sole operator and moderator of techpolicy.social, these technical requirements would be so cost- and time-prohibitive for me to implement that I would be forced to shut down techpolicy.social entirely. Additionally, because techpolicy.social can federate with other instances, I have no control over what content from techpolicy.social might appear on other instances, including instances that may have minor users. Although I try to carefully moderate the content on techpolicy.social and remove any objectionable and harmful content, I fear that I would

face liability under HB18 for any objectionable or harmful content that I mistakenly fail to remove and that appears on other instances that may have minor users.

9. Additionally, I understand that HB18 requires websites to “register” the ages of all users and then allow “verified” parents and guardians of minor children to inform the website that a user is a minor. *Id.* § 509.051. From there, websites must allow parents to control various aspects of their minor children’s accounts. *Id.* §§ 509.054, 509.102-03. I currently do not have any such mechanisms in place, and I understand that these mandatory mechanisms would require me to go to greater lengths to identify minor users than described above, in ¶ 5.a. These HB18-required processes would be cost-and time-prohibitive for a small website like mine to adopt. Below are two illustrative examples.

**a.** I will not be able to comply with Section 509.054’s requirement that I provide parental tools to verified parents of minors to supervise a minor’s use of techpolicy.social. Although I do not believe, to the best of my knowledge, that any known minors use techpolicy.social, it would be cost- and time-prohibitive to verify the ages of all techpolicy.social users and to create tools for parents to supervise a minor’s use of techpolicy.social.

**b.** HB18 also requires that I use a “commercially reasonable” method to verify that any alleged parent is the actual parent of an alleged minor. *Id.* § 509.101. Because the law does not define “commercially reasonable,” I do not know what verification methods comply with the law. Given this uncertainty and the large monetary awards for noncompliance, I would consider shutting down techpolicy.social rather than run the risk of violating the law.

10. In sum, the HB18 requirements discussed in this declaration are not the kinds of requirements that are possible to comply with for small websites like techpolicy.social: They are

too costly and time-intensive for websites with small operating teams—let alone sole proprietorships.

I declare under penalty of perjury, pursuant to 28 U.S.C. § 1746, that the foregoing is true and correct to the best of my knowledge.

Executed on July 26, 2024 in Tacoma, WA.



Chris Riley